Big data: A case study of disruption and government power

Galloway, Kathrine

Published in:
Alternative Law Journal

DOI:
10.1177/1037969X17710612

BIG DATA: A CASE STUDY OF DISRUPTION AND GOVERNMENT POWER

I. INTRODUCTION

History is replete with examples of government data collection to support taxation, and the targeted delivery of services, as well as repression. The advent of 'big data' however, has increased the scale, speed, and complexity of data collection and use to such an extent, that it is arguably qualitatively different from any analogue government record-keeping that has gone before it. If this assumption is correct, it represents a radical shift in the balance of power between state and citizen. Further, to the extent that the state is sharing data with the private sector, the boundaries of the exercise of power implicate corporations also.

This article first explains the upscaling of data collection to establish that it presents an entirely new capability for government. Certainly this has implications for privacy, surveillance, and the justice system, however the concern here is the shift in government activity that underlies these concerns. Embedding big data in government operations masks the deployment of big data as enhancing government power, rather than simply facilitating its execution. In other words big data is more than what is referred to as 'sustaining' technology it is disruptive.[1] For this reason, examination of the limits of government power is warranted.

To illustrate this argument, this article examines a selection of recent case studies of attempts by the Australian government to deploy big data as a tool of governance. It identifies the risk to the citizen inherent in the use of big data, to justify review of the bounds of government power in the face of rapid technological change.

II. BIG DATA

Historically data have been collected on paper—think the Domesday Book, and centuries of church registers recording births, deaths, and marriages—with attendant limitations on the application of that data. When only an original exists, and where copying involved travel to the site of that original and the skill of the transcriber, there was only a narrow scope for data sharing and matching.

This 'analogue' view represents a baseline understanding of the scope of government data collection. To the extent that data collection involves technology, the ordinary person might comprehend that it principally involves the storage and retrieval of data. Indeed government—and large corporations—are constrained in their collection of personal information, one form of data, through the operation of the *Privacy Act 1988* (Cth) which focuses on the access and control a person has over their own personal information, and the use to which personal information might be put. Within this framework, a privacy breach tends to be understood as an unauthorised accessing of personal information (with attendant misuse or disclosure) or perhaps a request for personal information where it is not warranted.

---

[1] 'Sustaining' and 'disruptive innovation' are terms coined by Clayton Christensen, *The Innovator's Dilemma* (Harvard Business School, 1997). Sustaining innovation permits us to the same work more efficiently, while disruptive innovation creates a new type of work altogether.

Exponential development in digital technologies has however, changed the data landscape. Technologies have not simply enhanced the efficiency of collection or storage of data: they make possible the generation of 'big data' and linkages across data sets that have previously not been possible. 'Big data' describes a huge data set that when analysed, affords insights into trends, patterns and associations, especially regarding human behaviour,[2] that would be impossible without technology. It is qualitatively different from 'ordinary' data collection—such as might be envisaged in an 'analogue' context—through three features: volume, variety, and velocity.[3] These characteristics refer to the sheer amount of data capable of collection, the number of types of data collected, and the speed of processing that data. These features permit big data to generate finely grained information about both niche and majority populations. Further, it supports the development of artificial intelligence that, amongst other things, permits predictions about the subjects of that data.[4] Applied also through time, the fact of this data, together with the capacity for advanced computational analysis and prediction, creates infrastructure with the ability to afford real-time understanding of populations and of individuals.

In the shift from analogue to digital, the advent of big data has expanded the capacity, scope, and purpose of government activity in a way that intrudes upon the citizen. Commentators have, for example, explored the complex issue of privacy,[5] and have identified the problems of surveillance.[6] Further, the application of artificial intelligence in the use of profiling—in criminal and terrorist activities—has attracted attention.[7]

While these inquiries are important in understanding the implications of big data in government, I suggest that there is an additional dimension of interest. The scope and potential of big data is so huge, that the way we understand information gathering and processing as a function of government is fundamentally altered. Consequently, we require a corresponding adjustment in the bounds of the exercise in government power both in the collection of data, and in its deployment.

I preface my comments by pointing out that technology is neither good nor bad. It can be applied to achieve any desired end. There is no reason to fear technology per se: but as a citizenry we must be cognisant of the implications of technology, including when it is put to use by government. So too must the law comprehend the pervasive application of data, including big data, in government activities.

---

[2] See eg Seref Sagiroglu and Duygu Sinanc, 'Big Data: A Review' (Paper presented at the International Conference on Collaboration Technologies and Systems (CTS), 2013) 42; C L Philip Chen and Zhang Chun-Yang, 'Data-Intensive Applications, Challenges, Techniques and Technologies: A Survey on Big Data' (2014) 275 (8/10/) *Information Sciences* 314.

[3] IBM, Paul Zikopoulos and Chris Eaton, *Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data* (McGraw-Hill Osborne Media, 2011), 5.

[4] Daniel E O'Leary, 'Artificial Intelligence and Big Data' (March-April 2013) *IEEE Intelligent Systems* 96.

[5] Xavier Fijac, 'Privacy and Self-management Strategies in the Era of Domestic Big Data' (2013) 32(3) *Communications Law Bulletin* 11.

[6] Melissa de Zwart, Sal Humphreys, Beatrix van Dissel, 'Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK' (2014) 37(2) *University of New South Wales Law Journal* 713.

[7] Lyria Bennett Moses and Janet Chan, 'Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools' (2014) 37(2) *University of New South Wales Law Journal* 643.

Further, there is no objection, within the norms of effective governance, natural justice, and the rule of law, to the collection of information per se. It is reasonable to assume that government can only really target and deliver services through at least some data collection, and that it may even be reasonable for government to link data in its control for the purpose of the execution of its lawful responsibilities. Where this has traditionally occurred through analogue processes, the inherent technological limitations of data collection have meant that the exercise of government power has been (arguably) effectively controlled through administrative law, including more recently, albeit weakly, through the *Privacy Act*. However, big data exponentially expands the possibilities or the scope of government operations—putting them beyond the contemplation of the existing framework of the law. This raises the question of whether existing curbs on executive power are sufficient to comprehend the exponentially greater power invested in government through big data.

III. COMMODITISATION OF DATA

Big data—rather than simply information about citizens or service users—is now assumed integral to government activity. This is clearly illustrated through the assumptions underlying the terms of reference of the Productivity Commission inquiry into data availability and use.[8] The inquiry will ascertain the 'costs and benefits of making more datasets available; examine options for data collection, sharing and release; identifying how consumers can benefit from access to data; and …consider how to preserve individual privacy and control over data use.' The Inquiry's terms of reference make a number of assumptions that are instructive in understanding institutional comprehension of big data.

The first assumption is that data is a valuable product. Certainly, data is now a commodity more than simply an expression of one's own information.[9] Framing the Inquiry around the costs and benefits of making *more* data available assumes that data is necessarily good, and it is economically important as a product on the open market.

The second assumption is that data should move freely. In other words, where one agency or firm holds data, that data should be available to other agencies and firms, who can draw on this information to offer better products or services for consumers and citizens. The flipside is that there is a cost associated with constraining data, and not sharing it freely. The argument seems to be that consumers will get inferior and perhaps more expensive products and services if agencies and firms do not have sufficient access to data to inform their operations.

The third premise underpinning the terms of reference is that all data are equal. The Inquiry focuses not only on private sector data (such as spending habits, or what people search for on the internet), but also on government data about citizens (income, health, education data, for example). The Inquiry is therefore to analyse the commodification of the data that we share or leave behind as consumers as well as the information we are required to give over to government. The idea of commoditisation of data effectively involves us both as consumers and as citizens,

[8] Productivity Commission, *Data Availability and Use* Draft Report (2016).
[9] See eg Paul M Schwartz, 'Property, Privacy, and Personal Data' (2003) 117 *Harvard Law Review* 2056.

becoming a product—or products given that data is aggregated.[10] Further, there is ostensibly a coming together of government and the private sector in collecting and sharing data about the citizen/consumer that represents a shift in power beyond government to include other institutions.

It is true that data—particularly big data—hold many benefits for the public. Public health, for example, is reliant on large datasets to gain insights into disease and its cause. There is a strong argument also for evidence-based government decisions and that evidence can be found through analysing huge amounts of data. However, the boundaries of government collection of data and its possible collaboration with the private sector are perhaps unclear.

This is more than a case of 'function creep'—data collection data for one purpose, but application towards additional purposes not originally envisaged. The possibility of convergence of all data, from all sources, appears to boost government power and with it, a validation of power exercised by corporations over the citizen. Without starting to examine questions of personal privacy arising from the purpose to which the data will be put, the fundamental issue in conceptual terms, is that of a breach of privacy through the initial collection and sharing of that data.

As evidenced by the terms of reference of the Productivity Commission Inquiry, government involvement in big data, and its commoditisation, appears to be assumed as a foundational position. These assumptions are reflected in recent misadventures in government deployment of its data and associated systems.

IV. GOVERNMENT DEPLOYMENT OF BIG DATA: CASE STUDIES

The Australian government's quest for agility and innovation in the face of digital disruption[11] has seen it embark on some high profile projects that highlight the need to question government relationship with big data. In particular, the following sections will analyse the 2016 census and the ongoing program of Centrelink data matching relating to social security recipients.

A. #Censusfail

In the lead up to the 2016 Census, the government was accused of function creep through plans to link the resulting data with data from other government agencies. Further, the Australian Bureau of Statistics ('ABS') also planned to link an individual's data from one Census into the future to gain a lifelong picture of that person. While the ABS has always provided a service of selling various datasets in various forms, it made clear that the additional functions would assist it to monetise the data collected.[12] Collectively, these changes represent a significant incursion into citizens' private lives.

---

[10] Yvonne de Souza, 'Not Just Data: Privacy in the Digital Age (2014) 60(5) *Feliciter* 17.
[11] Australian Government, *National Innovation and Science Agenda Report* (2015).
[12] Natasha Bita, 'Census 2016: ABS Bosses Discussed Secret Plans to Crossmatch Private Data' *Courier Mail* (online) 8 August 2016 <http://www.couriermail.com.au/news/census-2016-abs-bosses-discussed-plans-to-crossmatch-private-data/news-story/5770de257b4ab56a6a3039dad0e0bcfa>.

The first indicator of this incursion, arguably, was the ABS plan to retain names disclosed in the Census, with no destruction date.[13] In the face of criticism about the proposal, the ABS backed down, indicating that it would retain names until the earlier of 2020 or until no longer required.

One of the questions about the retention of names was whether they amounted to 'statistical information' for the purposes of s 8(3) of the *Census and Statistics Act 1905* (Cth) ('Act'). This provision reflects the power afforded by s 51(xi) of the *Australian Constitution* to enact legislation with respect to 'census and statistics'. The ABS website states that names are collected in the Census to[14] 'assist householders completing the form to report the relevant information for each person and to ensure the Census covers the entire population and data is of high quality.' Relevantly, the purpose of collecting names is to 'enhance the value of Census data, by combining it with other national datasets to better inform government decisions in important areas such as health, education, infrastructure and the economy.' This last purpose reflects the increasing importance of big data in government business.

On a reading of the statute however, names are not 'statistical information'. The stated purposes for collecting names are secondary to the purpose empowered under the Act and beyond the power afforded by the *Constitution*. It is a logical inconsistency to have a process by which to ascertain the entire population, yet relying on names to 'ensure that the Census covers the whole population.' If that entire population were already known (ostensibly by name) then there would be no need for a census. The purpose of collecting names arguably goes beyond even the permitted bounds of government power.

The second indicator of the creep of government power relates to privacy—although not only the potential loss of personal information once it is collected. The argument here is that a breach of privacy occurs at the very point of collection, regardless of how securely one's personal data is maintained.

Australia has no (or very limited) common law right to privacy[15] and has no bill of rights. There is therefore little systematic, strong protection for Australians against the exercise of State power through data collection.[16] It is therefore imperative that Australians do not easily give up any of the ad hoc protections they have; and that they are not required through force of law to empower State encroachment into personal freedoms. This is the most concerning aspect of the reach of the ABS through lateral and longitudinal data linkage.

---

[13] 'ABS Response to Privacy Impact Assessment' *Australian Bureau of Statistics Media Release*, 18 December 2015.

[14] Australian Bureau of Statistics, *About the Census*, 'Privacy, Confidentiality, Security' <http://www.abs.gov.au/websitedbs/censushome.nsf/home/privacy>.

[15] Australian Law Reform Commission, 'For Your Information: Australian Privacy Law and Practice' Report No 108 (2008); Australian Law Reform Commission, 'Serious Invasions of Privacy in the Digital Era' Report No 123 (2014), [3.53]-[3.58].

[16] The ABS has visibly exercised its power including via its field officers. Frequently individuals have perceived this – sometimes 'threatening' – exercise of power as sending a message that conflicts with the ABS's advertised position. See Kate Galloway, 'Troubles with #CensusFail' *Storify* (15 September 2016) <https://storify.com/katgallow/troubles-with-censusfail>.

Without entering into concerns about the potential for data breaches or the possibility of deployment for surveillance, through this system the State has removed Australians' individual capacity to establish and maintain boundaries between the State and citizen. This 'breathing space' would otherwise allow people to be themselves, guided by their social interactions and value systems, and free to become engaged citizens away from the gaze of the State. Becoming an engaged citizen is regarded by some as the very *nature* of privacy,[17] and by others as a *type* of privacy.[18] As Solove points out:

> The activities that affect privacy are not necessarily socially undesirable or worthy of sanction or prohibition. … In many instances, there is no clear-cut wrongdoer, no indisputable villain whose activities lack social value.[19]

Government promises to protect privacy are important, but miss an essential issue with the ABS plans for data linkage now available through big data: once we have given our information, our privacy has already been breached. Further, if the State demands our information under threat of punishment, citizens' privacy is breached before they have given over any information at all. By contrast, the State's understanding of 'privacy' suggests that it will protect us from interlopers' misuse of collected data without acknowledging that tracking citizens through their lives is a breach in the first place.[20]

While a discussion about privacy is important, it does not necessarily engage with the extent of government power to collect data in the first place, or the scope of the potential use of that data. In many cases, it focuses on the potential for unauthorised data leakage, for example, by hacking. Instead, I suggest that the advent of big data represents a qualitative shift in the very idea of information collection. To collect with the purpose in mind of data linkage, data aggregation, data mining, and artificial intelligence expands the reach of government power in ways not previously available in an analogue understanding of government activity, for purposes and through processes that are currently unknown and possibly unknowable. The asymmetry of power relations as between government and citizen means that the citizen cannot know how this data is going to be processed and used.[21]

Data collection and its aggregation and use as big data, challenges the foundational assumptions of the bounds of state power, and should therefore be addressed by policy-makers and Parliament before addressing additional questions of privacy once government has access to citizens' personal information.

---

[17] Julie E Cohen, Configuring the Networked Self: Law, Code and the Play of Every Day Practice (Yale University Press, 2012).
[18] Daniel J Solove, 'A Taxonomy of Privacy' (2006) 154 (3) *University of Pennsylvania Law Review* 477.
[19] Ibid 559.
[20] This point is made in the data retention context in Paul Bernal, 'DRIP: A Shabby Process for a Shady Law' *Paul Bernal's Blog: Privacy, Human Rights, Law, The Internet, Politics, More* (12 July 2014) <https://paulbernal.wordpress.com/2014/07/12/drip-a-shabby-process-for-a-shady-law/>.
[21] This is borne out by the increasing incidence of departmental releases of personal information to 'correct the record' following public criticisms of the Centrelink 'robo-debt' processes. See eg 'Editorial: Inhuman Services' *The Saturday Paper* (11 March 2017) <https://www.thesaturdaypaper.com.au/2017/03/11/inhuman-services/14891508004333>.

The third instructive feature of the Census incident is the adoption by the ABS of the language of efficiency and public interest in justifying the changes. This language reveals the government view of data collection as an activity that naturally falls within its scope. It implicitly acknowledges that change is afoot—otherwise the activity would not rate mention. It seeks to justify change however, without articulating the exponential shift in the nature and consequences of government data collection. It fails to mention the disruption to governance that is wrought by big data.

Adopting the language of neoliberalism has the ring of authority and 'common sense'. Who, after all, would seek inefficient government processes? However, while collecting and retaining our names along with our personal information may be efficient, this rationale for expansion of data collection does not address the foundation question of whether citizens retain the privacy that constitutes them as members of a liberal democratic society, or whether the collection of this information is a warranted exercise of state power. This is amplified because of the vastly expanded use to which data can now be put.

For all the preparation, obfuscation,[22] and justification of the ABS, on census night technology took its own course. Rather than a realisation of the scope of government power, the failure of the much-hyped online census form and the possibility of denial of service attacks on the ABS website, caused widespread public concern about the possibility of data breach—the 'privacy' issue that had attracted more widespread concern than the government's function creep. Yet the IT failure itself—attributed to budget cuts, lack of staff, lack of resources, and poor planning[23]—provides a further caution about government's entrée into big data. With the great power attendant upon contemporary and likely future data processing, comes the need for great skill as well as great responsibility. Neither of these were in evidence in #censusfail. Worryingly, there is further evidence that government remains ill-equipped to be trusted with data.[24]

B. Centrelink—#notmydebt

Following the disastrous foray into big data in the census, the public has become aware of what appears to be further government over-reach in data linking. Since December 2016, Australian media has been flooded with stories of people apparently wrongly subjected to Centrelink debt recovery processes.[25] Centrelink is Australia's department responsible for assessing and dispensing social security payments. As a consequence of its apparent wrong-headed deployment of big data, its customers are claiming that they are being wrongfully threatened with legal action for failure to pay debts that do not exist.

---

[22] The Senate Committee that investigated how the Census was conducted found that the changes warranted more public consultation and external scrutiny than it received, although it also confirmed that the ABS had not acted beyond its powers. See: Senate Economics References Committee, Parliament of Australia, *2016 Census: Issues of Trust* (2016), 38.

[23] Ibid.

[24] See eg Stilgherrian, 'Census Reports Highlight Government IT Incompetence' ZDNet (25 November 2016) <http://www.zdnet.com/article/census-reports-highlight-government-it-incompetence/>.

[25] #NotMyDebt (2016) <https://www.notmydebt.com.au/>.

Since mid-2016, Centrelink has matched its data with data held by the Australian Taxation Office ('ATO'). The intention, as stated by the Minister,[26] is to use it to uncover inconsistencies between what a person declares to Centrelink, and what they declare to the ATO. Centrelink can then use this information to recover any overpayment. However, the way government has set up the data linking is to match the fortnightly Centrelink payments against annual reported taxable income. The annual taxable income has been averaged over the year—with a high likelihood of an inaccurate picture of what a person received each fortnight through the year. For example, if a person was unemployed for six months and receiving benefits, but employed for the second six months in a high paying job, the six months of income will show up as averaged payments fortnightly for the entire year. That person will be asked to prove their Centrelink entitlement by producing pay slips for the period of employment. If unable to do so, Centrelink will claim repayment.

The result has been a large number of reported discrepancies that are readily explainable. Unfortunately for Centrelink clients however, the department requires payment within time limits that expire before the client can offer an explanation.

The Minister denies that there is a problem, reiterating that the system is doing what it was designed to do. He points out that it is recovering a lot of overpayments.[27] While this may be the case, this statement masks as much as it reveals. Many people for example, have indeed ultimately been found to owe some money. However according to the cases recorded on the website notmydebt.com.au, many who were initially charged with huge debts, sometimes thousands of dollars, were ultimately found to have owed only hundreds or very little at all. Further, because of the requirement to pay a 'debt' in advance of proving otherwise, it is anticipated that many people either failed to provide a defence, or were unable to. In these cases, the government will have recovered money by default without establishing entitlement to it.

There are of course, processes available for review of Centrelink debt assessments. However, customers have been told to commence repayment of the debt while they collect the evidence to disprove Centrelink's debt claim. This may consist of gathering pay slips from former employers, for example.

Centrelink's approach does two things: first, it places an immediate (and in many cases, unjustified or even incorrect) financial burden on the customer while secondly, placing the onus of proof of the absence of debt on the customer. In light of the likely vulnerability of so many of Centrelink customers, this is a heavy burden indeed.

Importantly, the government's deployment of big data processes fails here to meet criteria of natural justice and transparency that are a hallmark of good government. Natural justice requires a government decision-maker to make decisions that afford procedural fairness in carrying out their legislated responsibility.[28] While this does

---

[26] Sarah Martin, 'Welfare Debt Squad Hunts for $4bn in Over-payments' *The Weekend Australian* (online) 5 December 2016 <http://www.theaustralian.com.au/national-affairs/welfare-debt-squad-hunts-for-4bn-in-overpayments/news-story/e19c5b0d4a39aa07364a41269fdc11c9>.
[27] Joe Kelly, 'Alan Tudge Claims Labor's Centrelink Debt Victims Did Owe Money' *The Australian* (online) 26 January 2017 <http://www.theaustralian.com.au/national-affairs/alan-tudge-claims-labors-centrelink-debt-victims-did-owe-money/news-story/94f339427d94460d9b4f8127e919d1c1>.
[28] Robert Lindsay, 'Natural Justice: Procedural Fairness' (2011) 38(1) *Brief* 10, 13-14.

not mean necessarily that the resulting decision is fair, it does require fairness in the process by which that decision is made. Comments in the media, for example, will often cite the hardship of a client in having to repay money without establishing that the money is not in fact owed. My argument does not relate to these people, as difficult or tragic as some circumstances may be. Instead, it is the large proportion of people targeted, deliberately according to the Minister, by mismatched data that represents a breakdown in standards of governance.

Considering the number of claims Centrelink deals with annually, it is entirely likely that the Department or its algorithm will make mistakes. Procedural fairness then, would require that the customer have a clear process for having that decision reviewed according to law. Unlike the possibility of the odd human (or computer) error, what differs about the Centrelink situation is the scale of the issue—the volume characteristic of big data.

In the first place, Centrelink is now finding 20,000 debts a *week* instead of its previous (manually-determined) average of 20,000 debts a *year*.[29] Additionally, one Centrelink source is reported to have said that of 'the hundreds of cases they had reviewed, only about 20 (at a "generous estimate") turned out to be genuine debts.'[30] A huge increase in the number of debts and a significant proportion of those apparently 'false positives' points to a significantly flawed system, rather than a few outliers. Because of the scale of the problem, it might be said that the source of procedural unfairness lies within system for determining the debt in the first place.

To compound the issue of procedural fairness, the National Audit Office has found that 'nearly a quarter of the 57 million phone calls made to Centrelink [in 2014] went unanswered and that Australians spent 143 years waiting in vain to speak to Centrelink in 2013-2014, before simply hanging up…'[31] In other words, it is not easy to get in touch with the department if you have been issued with a demand to pay. For citizens who through disadvantage of one kind or another do not have the knowledge, resources, or resilience to battle the system, the consequences of an absence of procedural fairness are compounded.

Big data managed properly is entirely likely to bring benefits for government and citizen alike. But blindly following the lure of data without recognising the effects on human services and the foundations of the rule of law, interferes with the purpose of government itself at the cost of the citizen.

If the evidence about consumer experience of the Centrelink robo-debt program is true—and there certainly appears to be a lot out there—then it seems that the system is poorly designed to achieve its stated purpose of recovering money owed to the government. However, the Minister has been very clear—the system is working

---

[29] Christopher Knaus, 'Centrelink Officer Says Only a Fraction of Debts in Welfare Crackdown Are Genuine' *The Guardian* (online) 23 December 2016 <https://www.theguardian.com/australia-news/2016/dec/23/centrelink-officer-says-only-a-fraction-of-debts-in-welfare-crackdown-are-genuine>.
[30] Ibid.
[31] Noel Towell, 'Centrelink Blocks 60,000 Calls a Day, Blames Smartphone Apps' *Sydney Morning Herald* (online) 23 October 2015 <http://www.smh.com.au/it-pro/government-it/centrelink-blocks-60000-calls-a-day-blames-smartphone-apps-20151023-gkgmeo.html>.

exactly as it was designed to do so.[32] On this basis then, we must assume that the government has purpose-built a big data system that will incorrectly raise debts. In the absence of an accurate understanding of the boundaries of government power, there is no check on the potential abuse of the deployment of data.

In support of the argument that this is a question of governance, the former head of the government's Digital Transformation Office, Paul Shetler, has commented on the government's succession of IT failures—including #censusfail and Centrelink—describing them as 'cataclysmic' and 'not a crisis of IT' but a 'crisis of government'.[33]

The Centrelink debacle—in particular when viewed together with the government's other ill-conceived attempts at implementing digital services—demands an urgent and radical rethink about the nature of process of the exercise of state power in the face of pervasive digital technologies. To address this dissonance, Shetler has called for a 'radical upgrade' of IT skills in government. Similarly, Neuzerling attributes Centrelink's failure to 'data illiteracy'.[34] These assessments are entirely correct, although as intimated in Shelter's *Guardian* interview,[35] better digital capabilities must also pervade organisational culture. I would argue that beyond this, the law itself must clearly articulate the boundaries of state power in the face of digital transformation.

V. CONCLUSION

So is the government insufficiently competent to implement new technologies to serve the public? Or is it sufficiently competent to design a system that undermines natural justice in the exercise of government power? Either way, the law must hold government to account for the fallout.

Our complex and interconnected world functions on data. To gain the benefits data has to offer, there is a trade-off: a new kind of social contract. In exchange for giving up some of our privacy, we might have easy access to highly valuable goods and services. But we must also be clear about the costs—not costs to enterprise or government, and not only the economic costs to us as 'consumers'. We need to know the cost in terms of our relations with government itself.

The tussle between the exercise of executive power and the citizen's freedom and integrity is as old as government itself. Over centuries, our legal system has developed constraints on government action in recognition of the immense power it holds, and the adverse effects the exercise of naked power will have on the citizen.

---

[32] Stephanie Anderson and Henry Belot, 'Centrelink's Debt Recovery System Working, Human Services Minister Alan Tudge Says' *ABC News* (online) 11 January 2017 <http://www.abc.net.au/news/2017-01-11/centrelinks-debt-recovery-system-to-remain-government-says/8174644>.

[33] Christopher Knaus, 'Centrelink Crisis "cataclysmic" Says PM's Former Head of Digital Transformation' *The Guardian* (online) 6 January 2017 <https://www.theguardian.com/australia-news/2017/jan/06/centrelink-crisis-cataclysmic-turnbull-former-head-digital-transformation>.

[34] M D Neuzerling, 'Data Illiteracy is Causing Centrelink to Issue false Debts' *MDNeuzerling* (1 January 2017) <https://mdneuzerling.com/2017/01/01/data-illiteracy-is-causing-centrelink-to-issue-false-debts/>.

[35] Knaus, above n 32.

Consequently, we have developed a sophisticated understanding of the very nature of government—as an institution whose sole purpose is in service of the citizen.

Therefore, while government may be entitled to recover overpaid welfare payments, or may offer benefits through census data collection, it is not entitled to do so in a way that prejudices the wellbeing and freedoms of the citizen. As new tools come into existence—and in contemporary terms, these tools are digital technologies and big data—it is the responsibility of government to develop processes that harness these tools in the service of the citizen. Instead, we see their deployment as a crude exercise of power. Whether these tools have deliberately targeted citizens, or whether they have been deployed in ignorance, the ill-conceived Centrelink data matching process in particular demonstrates government that has lost its way. Yet whether government can be effectively constrained in its exercise of power is another question.

It is clear that until government grapples with the social, governance, and legal implications of digital technologies, the citizen remains at threat of unwarranted exercises of government power. This is indeed a ‘crisis of government’. It is now up to the public to make this a crisis *for* government (for all and any government) until the boundaries of power are recalibrated for a digital world.